Available at
www.ElsevierComputerScience.com
POWERED BY SCIENCE DIRECT®
Journal of Complexity 20 (2004) 245–265

Journal of COMPLEXITY

http://www.elsevier.com/locate/jco

Normal Boolean functions

Pascale Charpin

INRIA, Domaine de Voluceau, Rocquencourt, BP 105-78153, Le Chesnay Cedex, France

Received 19 November 2002; accepted 12 August 2003

Abstract

Dobbertin (Construction of bent functions and balanced Boolean functions with high nonlinearity, in: Fast Software Encryption, Lecture Notes in Computer Science, Vol. 1008, Springer, Berlin, 1994, pp. 61–74) introduced the *normality* of bent functions. His work strengthened the interest for the study of the restrictions of Boolean functions on k-dimensional flats providing the concept of k-normality. Using recent results on the decomposition of any Boolean functions with respect to some subspace, we present several formulations of k-normality. We later focus on some highly linear functions, bent functions and almost optimal functions. We point out that normality is a property for which these two classes are strongly connected. We propose several improvements for checking normality, again based on specific decompositions introduced in Canteaut et al. (IEEE Trans. Inform. Theory, 47(4) (2001) 1494), Canteaut and Charpin (IEEE Trans. Inform. Theory). As an illustration, we show that cubic bent functions of 8 variables are normal.

Keywords: Boolean function; Nonlinearity; Bent function; Almost optimal function; Resilient function; Normality; k-normality

1. Introduction

Normality was introduced by Dobbertin in [12]. Since this paper was mainly devoted to the construction of new bent functions, normality was defined for Boolean functions with an even number m of variables: such a function is normal if it is constant on some flat of dimension $m/2$. In particular, Dobbertin proposed the conjecture that any bent function is normal.

E-mail address: pascale.charpin@inria.fr.

0885-064X/$ - see front matter © 2003 Elsevier Inc. All rights reserved.
doi:10.1016/j.jco.2003.08.010

The known classes of bent functions, which are explicitely constructed, are normal. This leads to the main interest of normality concerning bent functions: *a bent function which is not normal does not belong to any known class of bent functions*. Since bent functions are not yet classified, normality appears as a relevant property. Recently, few examples of non-normal bent functions were exhibited using a specific algorithm. All these facts will be explained in forthcoming papers [6,11]. To find an infinite class of non-normal bent functions remains today an open problem.

The terminology was later extended to the odd case. Throughout a lot of observations and numerical results, it appears that normality is a property of a large class of Boolean functions. However Carlet proved in [8] that, asymptotically, almost all Boolean functions are not normal. Actually the general problem is *to find* k, *the larger dimension for an affine subspace such that a given function is constant on*, providing the concept of k-normality (see [8,13]). The complexity of any algorithm, which checks this property for a given function, strongly depends on the method which is used for the enumeration of all j-dimensional flats ($j \leqslant k$). Our aim, in this paper, is to establish some suitable simplifications by means of the decompositions of Boolean functions, a point of view that we developed with Canteaut et al. [4,5].

On the other hand we want to present and discuss some basic properties around the concept of normality for Boolean functions. Elementary aspects are presented in Section 2.2. The next section is devoted to the normality of any Boolean function viewed by its Fourier transforms. Here we want to show which formulas must be computed when checking the k-normality with respect to some flat (see Lemma 3). We after focus on a special class of Boolean functions including bent functions and almost optimal functions. Almost optimal functions provide classes of not normal functions (Theorem 1). We apply our results to the case of resilient functions in Section 3.1; we propose a sufficient condition, characterizing t-resilient functions which are not affine when at most $t+1$ variables are fixed (Theorem 2). In Section 3.2 as well as in the last section, we come back to highly non-linear functions. In accordance with our previous works, mainly in [4,5], we explain and develop the fact that to study the normality of bent functions (even case) is to study the normality of some almost optimal functions (odd case), notably by Propositions 5, 7 and 9. Concerning the bent functions we show that to consider such a function and its dual together should be more efficient (Proposition 6). We show that any cubic bent function of 8 variables is normal (Proposition 8). At the end, as an illustration, we treat the quadratic functions (in the Appendix).

Main notation:

- $\mathscr{B}_m$ is the set of Boolean functions of m variables;
- $wt(x)$ denotes the Hamming weight of the vector x;
- $\phi_E \in \mathscr{B}_m$ is the indicator of $E : \phi_E(x) = 1 \Leftrightarrow x \in E$;
- "$\cdot$" is the usual scalar product with respect to the standard basis;
- φ_a: $x \in \mathbf{F}_2^m \mapsto a \cdot x$, $a \in \mathbf{F}_2^m$, denotes any linear function in $\mathscr{B}_m$;
- $\mathscr{F}(f)$, $\mathscr{L}(f)$ and $\mathscr{N}(f)$, are defined by (1) and (2);
- $D_a f$ is the derivative of f with respect to a (see (3)).

2. Preliminaries

2.1. Boolean functions

We essentially use the same notation as [4,5]. A *Boolean function of m variables* is a function from $\mathbf{F}_2^m$ into $\mathbf{F}_2$, and we denote by $\mathscr{B}_m$ the set of all Boolean functions of m variables. Any $f \in \mathscr{B}_m$ can be expressed as a polynomial, called its *algebraic normal form* (ANF):

$$f(x_1, \ldots, x_m) = \sum_{u \in \mathbf{F}_2^m} \lambda_u \left(\prod_{i=1}^{m} x_i^{u_i} \right), \ \lambda_u \in \mathbf{F}_2.$$

The *degree* of f, denoted by $\deg(f)$, is the maximal value of $wt(u)$[1] such that $\lambda_u \neq 0$. Any Boolean function in $\mathscr{B}_m$ can also be identified with the binary codeword of length 2^m consisting of all values $f(x)$, $x \in \mathbf{F}_2^m$. By convention, the *weight of* f (i.e., the weight of the corresponding codeword of f) will be denoted by $\mathrm{wt}(f)$. The usual dot product between two vectors x and y is denoted by $x \cdot y$. We denote by $V^\perp$ the dual of any subspace $V \subset \mathbf{F}_2^m$ relatively to the usual scalar product:

$$V^\perp = \{x \in \mathbf{F}_2^m \mid \forall y \in V, \ x \cdot y = 0\}.$$

For any $a \in \mathbf{F}_2^m$, φ_a will denote the linear function in $\mathscr{B}_m : x \mapsto a \cdot x$. More generally, an *affine Boolean function* has the ANF:

$$\sum_{i=1}^{m} a_i x_i + \varepsilon, \ a_i \in \mathbf{F}_2, \ \varepsilon \in \mathbf{F}_2.$$

Note that, by convention, such a function can be constant.

The *Fourier transform* of $f \in \mathscr{B}_m$ in point a is denoted $\mathscr{F}(f + \varphi_a)$ and calculated as

$$a \in \mathbf{F}_2^m \mapsto \mathscr{F}(f + \varphi_a) = \sum_{x \in \mathbf{F}_2^m} (-1)^{f(x) + \varphi_a(x)}. \tag{1}$$

For convenience, $\mathscr{F}(f)$ will denote the Fourier transform in $a = 0$. Note that for any function $g \in \mathscr{B}_m$:

$$\mathscr{F}(g) = 2^m - 2wt(g).$$

The function g is said to be *balanced* if $wt(g) = 2^{m-1}$ or, equivalently, $\mathscr{F}(g) = 0$. Note that g is constant if and only if $\mathscr{F}(g) = \pm 2^m$.

The values of the Fourier coefficients $\mathscr{F}(f + \varphi_a)$ form the *Fourier spectrum* of f. The *non-linearity* $\mathscr{N}_f$ of f, which is the minimum value $wt(f + \varphi_a)$ when a describes $\mathbf{F}_2^m$, is related to the Fourier transform via following expression:

$$\mathscr{N}_f = 2^{m-1} - \frac{\mathscr{L}(f)}{2} \text{ where } \mathscr{L}(f) = \max_{a \in \mathbf{F}_2^m} |\mathscr{F}(f + \varphi_a)|. \tag{2}$$

[1] The *weight* of any binary vector $a = (a_1, \ldots, a_n) \in \mathbf{F}_2^m$ is the Hamming weight: $wt(a) = \sum_{i=1}^{n} a_i$. The vector u is written with the standard basis.

When m is even, it is known that $\mathscr{L}(f) \geqslant 2^{m/2}$ with equality for functions whose Fourier coefficients take the two values $\pm 2^{m/2}$ only—the so-called *bent functions*. When m is odd, any f satisfies $2^{m/2} < \mathscr{L}(f)$. For odd m such that $m < 9$, then $\mathscr{L}(f) \geqslant 2^{(m+1)/2}$ where equality holds for the so-called almost optimal functions (see Definition 6). It is a long-standing open problem to determine the exact lower bound for $m \geqslant 9$.

The *auto-correlation function* of $f \in \mathscr{B}_m$ refers to the mapping from $\mathbf{F}_2^m$ to the space of Boolean functions, $a \mapsto \mathscr{F}(D_a f)$, where

$$D_a f : x \mapsto f(x) + f(a + x) \tag{3}$$

is the *derivative* of f with respect to any direction $a \in \mathbf{F}_2^m$.

Definition 1. The *linear space* of any Boolean function f is the linear subspace of those elements a such that the function $D_a f$ is constant. Such nonzero a is called a linear structure of f.

Let E be any subset of $\mathbf{F}_2^m$. We denote by ϕ_E the Boolean function in $\mathscr{B}_m$ whose value on x is 1 if and only if $x \in E$; it is called *the indicator of* E. For any two functions f and g in $\mathscr{B}_m$, the function fg corresponds to the usual product in $\mathscr{B}_m$: $fg(x) = 1$ if and only if $f(x) = g(x) = 1$. For any $f \in \mathscr{B}_m$, the function $f\phi_E$ is called *the restriction of* f *to* E : $f\phi_E(x) = 1$ if and only if $f(x) = 1$ and $x \in E$. When V is a k-dimensional linear subspace of $\mathbf{F}_2^m$, the restriction of f to V, $f\phi_V$, can obviously be identified with a function of k variables. More generally, for any coset $b + V$ of V, we identify $f\phi_{b+V}$ with $f_b \in \mathscr{B}_k$ as follows: $f_b(x) = f(x + b), x \in V$. Note that the function $f_b \in \mathscr{B}_k$ is defined up to any translation $x \mapsto x + v$, $v \in V$. In general, the properties studied in this paper are invariant under translations.

Definition 2. Let $f \in \mathscr{B}_m$ and let V be a linear subspace of $\mathbf{F}_2^m$ of dimension k. The *decomposition of* f *with respect to* V is the sequence $\{f_b,\ b \in W\}$ where $V \times W = \mathbf{F}_2^m$ and $f_b = f\phi_{b+V}$, by identifying $f\phi_{b+V}$ to a Boolean function in $\mathscr{B}_k$.

The following properties, describing the links between f and its restrictions, will be intensively used in this paper. They are usually known; proofs can be found in [3, 4, Section V; 5].

According to the previous definition, we have for any decomposition of f with respect to some k-dimensional subspace V:

$$\sum_{v \in V^\perp} \mathscr{F}^2(f + \varphi_v) = 2^{m-k} \sum_{b \in W} \mathscr{F}^2(f_b), \tag{4}$$

where f_b is the restriction of f to $b + V$. The following properties are directly deduced:

$$\text{For all } b \in W,\ \mathscr{L}(f_b) \leqslant \mathscr{L}(f), \tag{5}$$

$$\sum_{b \in W} \mathscr{F}^2(f_b) \leqslant \mathscr{L}^2(f). \tag{6}$$

On the other hand, let us denote by $f\circ\tau_b$, $b\in W$, the Boolean function in $\mathscr{B}_m$ defined by $f\circ\tau_b(x)=f(x+b)$. Then we have

$$\sum_{v\in V^\perp}\mathscr{F}(f\circ\tau_b+\varphi_v)=\sum_{v\in V^\perp}(-1)^{b\cdot v}\mathscr{F}(f+\varphi_v)=2^{m-k}\mathscr{F}(f_b). \tag{7}$$

For $b=0$, (7) is simply

$$\sum_{v\in V^\perp}\mathscr{F}(f+\varphi_v)=2^{m-k}\sum_{x\in V}(-1)^{f(x)}=2^{m-k}\mathscr{F}(f_0), \tag{8}$$

where f_0 denotes the restriction of f to V. Note that for simplicity (and if there is no confusion about the choice of the decomposition), we will often write the decomposition of f with respect to V as $f=(f_1,\ldots,f_t)$, with $f_i\in\mathscr{B}_k$ and $t=2^{m-k}$.

2.2. Introduction of normality

The concept of normality was introduced by Dobbertin for even m [12]. Our terminology here follows more recent works as [8,13]. Note that $\lceil m/2\rceil$ is equal to $m/2$ for even m and to $(m+1)/2$ for odd m. Recall that, by convention, an *affine* function f is such that $deg(f)\leqslant 1$.

Definition 3. A Boolean function $f\in\mathscr{B}_m$ is said to be *normal* when it is constant on an affine subspace U of $\mathbf{F}_2^m$ of dimension $\lceil m/2\rceil$. In this case f is said to be *normal with respect to* U.

The function f is said *weakly normal* when it is affine, and not constant, on a flat U of dimension $\lceil m/2\rceil$.

The normality is connected with the problem of the determination of the highest dimension of the affine space where f is constant.

Definition 4. A Boolean function $f\in\mathscr{B}_m$ is said to be *k-normal*, $k\leqslant m$, if there exists a k-dimensional flat on which f is constant. It is weakly k-normal if it is affine, and not constant, on some k-dimensional flat.

Suppose that f is weakly normal with respect to U; so the restriction of f to U can be identified to some affine function $\ell\in\mathscr{B}_{\lceil m/2\rceil}$. Then there is v such that $f+\varphi_v$ is normal on U—by choosing v such that the restriction of φ_v to U is either ℓ or $1+\ell$. Conversely, if f is constant on U then the function $f+\varphi_v$ is either constant or affine on U for any v. More precisely, set $U=a+V$ where V is a subspace of dimension $\lceil m/2\rceil$ and $a\in\mathbf{F}_2^m$. Consider $\varphi_v(x)=v\cdot x$ for $x\in a+V$; the restriction of φ_v to $a+V$ is not constant if and only if $y\in V\mapsto v\cdot(a+y)$ is not constant, i.e. $y\mapsto v\cdot y$ is not null or, equivalently, $v\notin V^\perp$. We claim that *f is normal if and only if some function of its*

spectrum is weakly normal and we precise which functions are weakly normal. This result is obviously generalized as follows:

Lemma 1. *Let $f \in \mathscr{B}_m$. Then f is k-normal with respect to U, if and only if there is $v \in \mathbf{F}_2^m$ such that $f + \varphi_v$ is affine on U. When $v \notin V^\perp$, where V denotes the subspace which has U as a coset, then $f + \varphi_v$ is affine and not constant on U.*

It is important to notice that the property for a function of m variables *to be constant on some flat* holds up to the automorphism group of the Reed–Muller code of order one and length 2^m. Indeed this automorphism group is the *general affine group*, usually denoted by $AGL(m, 2)$. It is the group generated by the linear permutations and by the *translations* on $\mathbf{F}_2^m$ (we call *translations* the mappings $x \mapsto a + x,\ a \in \mathbf{F}_2^m$). The set of the affine subspaces of $\mathbf{F}_2^m$ is clearly invariant under all these permutations.

Lemma 2. *Let $f \in \mathscr{B}_m$. Denote by σ any linear permutation on $\mathbf{F}_2^m$. If f is constant on some affine subspace of $\mathbf{F}_2^m$ then*

- *the functions of type $f(\sigma(x) + a),\ x = (x_1, \ldots, x_m)$ and $a \in \mathbf{F}_2^m$, satisfy this property too;*
- *the function $f + 1$ satisfies this property too.*

Throughout a lot of observations and numerical results, and as we will see in this paper, it is easy to characterize infinite classes of normal functions while it is difficult to prove that a function is not normal. As an illustration the following example leads immediately to general results.

Example 1. Let $f \in \mathscr{B}_{10}$, given by its ANF:

$$f(x) = x_1x_2x_3x_4x_5 + x_6x_7x_8x_9x_{10} + x_1x_2 + x_3x_4 + x_6x_7 + x_8x_9 + x_{10}.$$

Let V be the subspace of dimension 5, defined by $x_2 = x_4 = x_7 = x_8 = x_{10} = 0$. Each term of f contains at least one $x_i,\ i \in \{2, 4, 7, 8, 10\}$. This implies

$$f(x_1, 0, x_3, 0, x_5, x_6, 0, 0, x_9, 0) = 0,\ \forall x.$$

Then f is normal with respect to V, since $f\phi_V = 0$.

Actually the previous example refers to an obvious property. Consider $f \in \mathscr{B}_m$ which has an ANF of the form

$$f(x_1, \ldots, x_m) = x_1A_1 + \cdots + x_tA_t, \tag{9}$$

where $t = m/2$ for even m and $t = (m - 1)/2$ for odd m and each A_i denotes the ANF of some Boolean function of the $m - 1$ variables $\{x_j | 1 \leqslant j \leqslant m,\ j \neq i\}$. Then f is

normal with respect to V, the subspace defined by

$$x_1 = \cdots = x_t = 0.$$

This method can be applied more generally or, precisely, for quadratic functions as we will see later (in the Appendix). There is actually a general result which is easily deduced from the representation of a given Boolean function by its ANF.

Proposition 1. *Let us denote by k some integer in the range $[1, m]$. Let $f \in \mathscr{B}_m$ such that its ANF is of the following form*:

$$f(x_1, \ldots, x_m) = \sum_{\substack{u \in \mathbf{F}_2^m \\ wt(u) > k}} \lambda_u \left(\prod_{i=1}^{m} x_i^{u_i} \right) \text{ with } \lambda_u \in \mathbf{F}_2.$$

Then f is k-normal, equal to zero, with respect to any subspace V defined by

$$x_{i_1} = \cdots = x_{i_{m-k}} = 0 \text{ where } 1 \leqslant i_j \leqslant m.$$

Proof. Each term in the ANF of f is of degree strictly greater than k. So each term is zero if at least $m - k$ variables are zero. □

Example 2. Let m be odd and let the symmetric function

$$f(x_1, \ldots, x_m) = \sum_{u, wt(u) = (m+3)/2} \left(\prod_{i=1}^{m} x_i^{u_i} \right).$$

According to Proposition 1 (with $k = (m+1)/2$), f is normal with respect to any subspace V of dimension $(m+1)/2$ defined by $x_{i_1} = \cdots = x_{i_{(m-1)/2}} = 0$.

Clearly, any function whose ANF has no monomials of degree 1, 2 and 3 is constant on a subspace of dimension 3. But more is known: *for $m \geqslant 4$ any Boolean function is* 2*-normal* and *for $m \geqslant 6$ any Boolean function is* 3*-normal* [2]. This result, is based on the work of Dubuc [13] who proved:

Proposition 2. *For $m \leqslant 7$, any Boolean function of m variables is $\lfloor m/2 \rfloor$-normal.*

3. Normality and Fourier coefficients

In this section, our aim is to characterize normal functions, especially when these functions are highly non-linear. We first use intensively the formulas of Section 2.1 in order to state precisely what means k-normal, which properties could simplify algorithms or allow us to obtain full results on special classes. We then propose a general characterization which we apply to the class of resilient functions. The next

sections are devoted to (almost) optimal functions. In the next lemma we distinguish normality with respect to any subspace and normality with respect to any affine subspace, for clarity.

Lemma 3. *Let $f \in \mathcal{B}_m$ and let V be any subspace of dimension k. Consider the sums*:

$$S_a = \sum_{v \in V^\perp} \mathcal{F}(f + \varphi_{a+v}),\ a \in W,\ V^\perp \times W = \mathbf{F}_2^m.$$

The function f is affine on V if and only if there is $b \in W$ such that $S_b = \pm 2^m$. In this case, $S_a \in \{0, \pm 2^m\}$ for all a and $f + \varphi_b$ is k-normal with respect to V (such b is unique).

More generally, the function f is affine on $c + V$, $c \notin V$, if and only if one of the sums

$$T_{a,c} = \sum_{v \in V^\perp} (-1)^{c \cdot v} \mathcal{F}(f + \varphi_{a+v}),\ a \in W,\ V^\perp \times W = \mathbf{F}_2^m,$$

say $T_{b,c}$, equals $\pm 2^m$. In this case, $T_{a,c} \in \{0, \pm 2^m\}$ for all a and $f + \varphi_b$ is k-normal with respect to $c + V$.

Proof. Let us denote by h the restriction of f to V. According to (4), $S_a = 2^{m-k} \mathcal{F}(h + \ell_a)$ where ℓ_a is the restriction of φ_a to V. Note that

$$\mathcal{F}(h + \ell_a) = \sum_{x \in V} (-1)^{f(x) + a \cdot x} \text{ where } a \notin V^\perp.$$

So we get here, when a describe W, the 2^k Fourier coefficients of h. But h is affine if and only if one of these coefficients equals $\pm 2^k$. More precisely, if h is affine only one among these coefficients is $\pm 2^k$ and any other is 0. The function $f + \varphi_b$ corresponding to $\mathcal{F}(h + \ell_b) = \pm 2^k$ is constant on V.

The general case is obtained by applying (7)—i.e. f is affine on $c + V$ if and only if the function $x \mapsto f(x + c)$ is affine on V. □

The complexity of any algorithm checking if a given function is k-normal (or not) strongly depends on the method which is used for the enumeration of all k-dimensional flats. By the previous lemma, we only want to explain what must be checked for any given subspace in order to establish some suitable simplifications. Our method can be summarized as follows:

The function f is given by its Fourier-spectrum; notation is as Lemma 3.

For any k-dimensional subspace V
  For any $c \in W'$, $V \times W' = \mathbf{F}_2^m$,
    For any a compute $T_{a,c}$;
If $T_{a,c} \notin \{0, \pm 2^m\}$ then f is not affine on $c + V$ else
If $T_{a,c} = \pm 2^m$ then f is affine on $c + V$ and $f + \varphi_a$ is k-normal with respect to $c + V$.

Now we focus on a special class of functions which includes highly non-linear functions.

Theorem 1. *Let $f \in \mathcal{B}_m$ and let k be an integer such that $m/2 \leqslant k \leqslant m$.*

If f is k-normal (or weakly k-normal) then $2^k \leqslant \mathcal{L}(f)$.

Assume that $\mathcal{L}(f) = 2^k$. Let us denote by V, any subspace of dimension k and by $b + V$ some coset of V. Then

- *f is constant on $b + V$ if and only if*

$$(-1)^{b\cdot v}\mathcal{F}(f + \varphi_v) = \varepsilon 2^k, \ \forall v \in V^{\perp}, \tag{10}$$

  where ε is constant, equal either to 1 or to -1;
- *if f is such that $|\mathcal{F}(f)| < 2^k$ then f is not k-normal;*
- *if f is constant on some coset of V then f is balanced on all other cosets of V.*

Proof. The function f is k-normal if and only if some function of its spectrum is weakly k-normal (according to Lemma 1). So we can assume that f is k-normal with respect to U. Let h denote the restriction of f to U. According to (5) we have $\mathcal{L}(h) \leqslant \mathcal{L}(f)$ where $\mathcal{L}(h) = 2^k$, then $2^k \leqslant \mathcal{L}(f)$.

From now on f is such that $\mathcal{L}(f) = 2^k$. According to (7), f is constant on $b + V$ if and only if

$$\sum_{v \in V^{\perp}} (-1)^{b\cdot v}\mathcal{F}(f + \varphi_v) = 2^{m-k}\mathcal{F}(f_b) = \pm 2^m,$$

where f_b denotes the restriction of f to $b + V$. Since $|\mathcal{F}(f + \varphi_v)| \leqslant 2^k$ for all v, this property holds if and only if the 2^{m-k} terms in the sum above have the same value $\varepsilon 2^k$ where $\varepsilon = 1$ if the sum is equal to 2^m and $\varepsilon = -1$ otherwise. Obviously, $|\mathcal{F}(f)| < 2^k$ contradicts (10).

Now, denote by $\{f_a, \ a \in W\}$ the decomposition of f with respect to V, where $V \times W = \mathbf{F}_2^m$. If f is constant on $b + V$, for some b, then $\mathcal{F}^2(f_b) = 2^{2k}$ and, applying (6), we obtain

$$2^{2k} \leqslant \sum_{a \in W} \mathcal{F}^2(f_a) \leqslant 2^{2k}.$$

Thus $\mathcal{F}(f_a) = 0$ for any $a \neq b$, completing the proof. □

Remark 1. The property $\mathcal{L}(f) \geqslant 2^k$ means that the non-linearity $\mathcal{N}_f$ of f satisfies $\mathcal{N}_f \leqslant 2^{m-1} - 2^{k-1}$, by definition of $\mathcal{N}_f$. It is well-known that any $f \in \mathcal{B}_m$ satisfies $\mathcal{L}(f) \geqslant 2^{m/2}$; hence this bound is significant for $k \geqslant m/2$ only.

Note that the second result of Theorem 1 is obviously deduced but surprising, since it provides non-normal functions. For instance, *any balanced function f such that $\mathcal{L}(f) = 2^k$ is not k-normal*. In particular, *resilient functions* are balanced and can satisfy the hypothesis of Theorem 1.

The third result implies that if f is neither constant nor balanced on V then f is not constant on any coset of V.

3.1. On resilient functions

A function $f \in \mathscr{B}_m$ is said to be *t-resilient* if $\mathscr{F}(f+\varphi_a)=0$ for all a satisfying $wt(a)\leqslant t$. By convention, such a function is not affine. Moreover, in order to define resilient functions, we assume that functions are represented by their ANF, after fixing the standard basis. Actually the resiliency was first introduced as follows by Siegenthaler [19]: f is said to be *t-resilient* if, by fixing any set of r variables, where $r\leqslant t$, the function f, considered as a function of $m-r$ variables, is always a balanced function. More precisely:

Definition 5. Let $f \in \mathscr{B}_m$ which is expressed by its ANF with respect to the standard basis. Let us define, for any $a \in \mathbf{F}_2^m$, the subspace whose dimension is the weight $wt(a)$ of a:

$$V_a = \{u \in \mathbf{F}_2^m \mid u \preccurlyeq a\}$$

where $u \preccurlyeq a$ means that $u_i \leqslant a_i$ for all i—i.e. a covers u. Setting $a=(a_1,\ldots,a_m)$, we denote by $\bar{a}$ the vector $(a_1+1,\ldots,a_m+1)$.

The function f is t-resilient if for any a such that $wt(\bar{a})\leqslant t$ every restriction of f to every coset of V_a is balanced.

We are going to examine the following problem: on which flat, defined by fixing some variables, a given resilient function is (or not) affine?

Theorem 2. *Let $f \in \mathscr{B}_m$ be a t-resilient function $(1\leqslant t\leqslant m-3)$ which is not $t+1$-resilient. For $a \in \mathbf{F}_2^m$, set $\bar{a}=(a_1+1,\ldots,a_m+1)$; the subspace V_a is explained by Definition 5. We have:*

(i) *Assume that f is such that $\mathscr{F}(f+\varphi_v)\neq 0$ for all v such that $wt(v)=t+1$. Then for all a such that $wt(\bar{a})\leqslant t+1$ f is not affine on any coset of the k-dimensional subspace V_a $(k\geqslant m-(t+1))$.*

(ii) *More precisely, let a such that $wt(\bar{a})\leqslant t+1$. If $\mathscr{F}(f+\varphi_{b+\bar{a}})\neq 0$ for some $b\in V_a$ satisfying $wt(b+\bar{a})=t+1$ then f cannot be affine on any coset of V_a.*

Especially, when $wt(\bar{a})=t+1$ then f is not affine on any coset of V_a if $\mathscr{F}(f+\varphi_{\bar{a}})\neq 0$.

Proof. Note that $wt(\bar{a})\leqslant t+1$ means $wt(a)\geqslant m-(t+1)$; in this case the dimension of V_a is greater than or equal to $m-(t+1)$. Clearly

$$V_a^{\perp} = \{v \mid v \preccurlyeq \bar{a}\} = V_{\bar{a}},$$

for any a. Moreover we have here $V_a \times V_{\bar{a}} = \mathbf{F}_2^m$. We apply Lemma 3, considering for any $b \in V_a$ and for any $c \in V_{\bar{a}}$ the sum

$$T_{b,c} = \sum_{v \preccurlyeq \bar{a}} (-1)^{c \cdot v} \mathscr{F}(f + \varphi_{b+v}).$$

Let a be such that $wt(a) \geqslant m - t - 1$; thus $wt(\bar{a}) \leqslant t + 1$. As f is t-resilient, we know that $\mathscr{F}(f + \varphi_v) = 0$ for all v such that $wt(v) \leqslant t$. In particular $T_{0,c} = 0$ for all c when $wt(\bar{a}) \leqslant t$. Suppose that there is $b \in V_a$ such that $wt(b + \bar{a}) = t + 1$ and $\mathscr{F}(f + \varphi_{b+\bar{a}}) \neq 0$, providing for each $c \in V_{\bar{a}}$:

$$T_{b,c} = (-1)^{c \cdot \bar{a}} \mathscr{F}(f + \varphi_{b+\bar{a}}) \neq 0.$$

Note that for $wt(\bar{a}) = t + 1$ our hypothesis becomes $\mathscr{F}(f + \varphi_{\bar{a}}) \neq 0$ (and $b = 0$). As f is not constant, we conclude that $T_{b,c} \notin \{0, \pm 2^m\}$, for all c. According to Lemma 3, the proof of (ii) is completed and (i) is directly deduced. □

Many resilient functions $f \in \mathscr{B}_m$ are effectively constructed by concatenating several functions of $\mathscr{B}_k$, $k \leqslant m$. The choice of these functions is important considering other cryptographic properties. For instance the so-called Maiorana–McFarland functions, which provide the largest known class of resilient functions were introduced in [1] as concatenations of affine functions, by fixing some variables (see, for instance, the recent papers [9], [10, Section 6]). The previous proposition has concern with other kinds of resilient functions, especially when the order t of resiliency is high (i.e. $m - t$ is small).

Open problem 1. *Construct t-resilient functions with t as high as possible satisfying, for such a function f : $\mathscr{F}(f + \varphi_v) \neq 0$ for all v such that $wt(v) = t + 1$.*

Any t-resilient function f satisfies $\mathscr{L}(f) \geqslant 2^{t+2}$ [18]. When $\mathscr{L}(f) = 2^{t+2}$ then the degree of f is as high as possible since it is exactly $m - t - 1$ (from the Siegenthaler's bound [19]); moreover the Fourier spectrum of f is $\{0, \pm 2^{t+2}\}$ [20] (f is *three-valued*). *Such a t-resilient function is said to achieve the best nonlinearity* [9]. Since it is balanced, such a function is not $(t + 2)$-normal (from Theorem 1). But these functions could be affine on some k-dimensional flat. For instance, take $t = (m - 3)/2$ with odd m and consider t-resilient functions with the best non-linearity. Such a function f is of most interest since it is highly non-linear ($\mathscr{L}(f) = 2^{(m+1)/2}$), highly resilient and has an high degree $m - t - 1 = (m + 1)/2$. According to Theorems 1 and 2, we express as follows the fact that by fixing at most $(m - 1)/2$ variables in the ANF of f we cannot obtain an affine function.

Corollary 1. *Let $f \in \mathscr{B}_m$, m odd, be a $((m - 3)/2)$-resilient function such that $\mathscr{L}(f) = 2^{(m+1)/2}$. Let us consider the subspaces*

$$V_a = \{u \in \mathbf{F}_2^m \mid u \preccurlyeq a\}, \ wt(a) \geqslant (m + 1)/2.$$

Assume that $\mathscr{F}(f + \varphi_v) \neq 0$ for all v such that $wt(v) = (m - 1)/2$. Then f is not affine on any flat $b + V_a$, for all b and for all a. Therefore f is neither normal nor weakly

normal with respect to any coset of V_a such that $wt(a) = (m+1)/2$ (here the dimension of V_a is exactly $(m+1)/2$).

Example 3. Set $m = 7$; let $f \in \mathscr{B}_7$ be a 2-resilient function. Then $deg(f) \leqslant 4$ from Siegenthaler's bound. By definition, f is balanced on the subspaces

$$V_a = \{u \in \mathbf{F}_2^m \mid u \preccurlyeq a\}, \ \ wt(a) \in \{5, 6\}$$

(of codimension 1 and 2) and on their cosets. Now suppose that $\mathscr{F}(f + \varphi_v) \neq 0$ for all v such that $wt(v) = 3$. In accordance with Theorem 2, f is not affine on V_a and on its coset, for all a such that $wt(a) \geqslant 4$.

3.2. Almost optimal functions—for odd m

Theorem 1 is of most interest for functions such that $\mathscr{L}(f) = 2^{\lceil m/2 \rceil}$, since in this case it has concern with the *normality*, as given by Definition 3. We will now focus on these functions; we begin by recalling the definition of *almost optimal functions*; these functions were extensively studied in [4].

Definition 6. The Boolean function $f \in \mathscr{B}_m$ is said to be almost optimal if

- $\mathscr{L}(f) \leqslant 2^{(m+2)/2}$, when m is even;
- $\mathscr{L}(f) \leqslant 2^{(m+1)/2}$, when m is odd.

The function f is said to be three-valued almost optimal if its Fourier spectrum is $\{0, \pm 2^{(m+2)/2}\}$ when m is even and $\{0, \pm 2^{(m+1)/2}\}$ when m is odd.

In this section, we treat the odd case; for almost optimal functions, our previous results have immediate consequences.

Corollary 2. *Let $f \in \mathscr{B}_m$, m odd, be an almost optimal function. Then*:

(i) *If f is balanced then f is not normal.*
(ii) *If $\mathscr{L}(f) < 2^{(m+1)/2}$ then $f + \varphi_v$ is not normal, for any v.*
(iii) *Assume that $\mathscr{L}(f) = 2^{(m+1)/2}$. Let N be the number of v such that $|\mathscr{F}(f + \varphi_v)| = \mathscr{L}(f)$. If $N < 2^{(m-1)/2}$ then $f + \varphi_v$ is not normal, for any v.*

Proof. It is important to notice that the hypothesis on f, in each statement (ii) and (iii), holds for any function $f + \varphi_v$ of the spectrum of f. So we need to prove these results for f only.

If $\mathscr{L}(f) < 2^{(m+1)/2}$, we know from Theorem 1 that f cannot be k-normal with $k = (m+1)/2$. As $(m+1)/2 = \lceil m/2 \rceil$, this is to say "$f$ is not normal". We suppose now that $\mathscr{L}(f) = 2^{(m+1)/2}$. From Theorem 1 again (with $k = (m+1)/2$), if f is balanced then it cannot be normal, so that (i) is proved. Assuming that $\mathscr{F}(f) \neq 0$, if f

is normal then there are at least $2^{(m-1)/2}$ functions $f+\varphi_v$ such that the absolute value of $\mathscr{F}(f+\varphi_v)$ is equal to $2^{(m+1)/2}$ (from (10)). This contradicts $N<2^{(m-1)/2}$. □

There are important classes of almost optimal functions. We studied such a class in the previous section (Corollary 1). Another example is the class of *partially bent functions*[2] which are almost optimal. Up to affine transformations on the variables, such a function f has an ANF of the following form:

$$f(x_1, \ldots, x_m) = g(x_1, \ldots, x_{m-1}) + \varphi_b(x_1, \ldots, x_m), \tag{11}$$

where g is a bent function of $m-1$ variables and φ_b is some linear function. When it is quadratic, f is at least weakly normal (see Theorem 4). Otherwise, it is clear that the normality of f is connected with the normality of the bent function g—another general problem. Partially bent functions arise in the next proposition, a small extension of Proposition 2. Note that the concept of *linear structure* is defined in Section 2.1 (see Definition 1).

Proposition 3. *For $m=7$, any function $f\in\mathscr{B}_7$ which has a linear structure, say a, is either weakly normal or normal; it is normal if the function D_af is null, especially when f is not balanced.*

In particular, any partially bent function which is almost optimal (i.e., *of form* (11)) *is normal when it is not balanced and weakly normal otherwise.*

Proof. Let $f\in\mathscr{B}_7$ be such that the function D_af is constant for some a. Let H be an hyperplane which does not contain a. Let $f=(g,h)$ be the decomposition of f with respect to H, with $g(x)=f(x)$ and $h(x)=f(x+a)$ for $x\in H$ (see Definition 2). Then, since $D_af(x)=f(x)+f(x+a)$, the decomposition of D_af with respect to H is

$$D_af=(g+h, g+h), \text{ with } D_af\in\{0,1\}.$$

This implies that $g=h+\varepsilon$ where $\varepsilon=0$ when $D_af=0$ and $\varepsilon=1$ otherwise. Therefore $f=(g, g+\varepsilon)$. As g can be identified to a Boolean function of 6 variables, it is constant on some three-dimensional flat U. So f is either normal with respect to $U\cup(a+U)$, if $\varepsilon=0$, or weakly normal with respect to $U\cup(a+U)$ otherwise. Note that $D_af=1$ implies that f is balanced.

Now suppose that f is equivalent to a function given by (11), up to affine transformations. Thus f has a linear structure, $a=(0,\ldots,0,1)$, implying that f is normal when it is not balanced. Moreover f is such that $\mathscr{L}(f)=2^{(m+1)/2}$. So according to Corollary 2, if f is balanced it is not normal, completing the proof. □

As we recall by the next example, there are functions satisfying the hypothesis of Corollary 2(ii). There exist also functions which are almost optimal and not

[2] The partially bent functions, introduced by Carlet [7], are notably studied in [4]. These functions are three-valued and some are almost optimal.

three-valued (see [14]), but we do not know any function satisfying the hypothesis of Corollary 2(iii).

Open problem 2. *Does it exist $f \in \mathscr{B}_m$, for odd m, such that $\mathscr{L}(f) = 2^{(m+1)/2}$ and*

$$\mathtt{card}\{v \in \mathbf{F}_2^m \mid \mathscr{F}(f+\varphi_v) = \pm 2^{(m+1)/2}\} < 2^{(m-1)/2}.$$

Example 4. Applying Corollary 2(ii), we can exhibit examples of functions which are not normal. In [17], two functions f of $\mathscr{B}_{15}$ are given which satisfies:

$$\mathscr{L}(f) = 216 \text{ while } 2^{(m+1)/2} = 2^8 = 256.$$

Such a function is not normal as well as any function belonging to its spectrum.

Any three-valued almost optimal function $f \in \mathscr{B}_m$, m odd, has the following Fourier spectrum (see a proof in [5]):

$\mathscr{F}(f+\varphi_u)$	Number of $u \in \mathbf{F}_2^m$
0	2^{m-1}
$2^{(m+1)/2}$	$2^{m-2} + (-1)^{f(0)} 2^{(m-3)/2}$
$-2^{(m+1)/2}$	$2^{m-2} - (-1)^{f(0)} 2^{(m-3)/2}$

We will see later that these functions are strongly connected with the bent functions of $m \pm 1$ variables. More precisely we claim that *any property concerning three-valued almost optimal functions has concern with bent functions*. Our interest is here for normality and the main problem is:

Open problem 3. *Characterize a class of three-valued almost optimal functions which have no weakly normal function in their spectrum.*

In this context, the set of u such that $\mathscr{F}(f+\varphi_u) = 0$ could have suitable combinatorial properties. For instance, the next proposition is simply deduced from Theorem 1. Considering (10) for $k = (m+1)/2$, the dimension of $V^\perp$ is $(m-1)/2$. If f is normal with respect to some coset of V then $\mathscr{F}(f+\varphi_v) \neq 0$, for all $v \in V^\perp$. Suppose that an odd number of the coefficients $\mathscr{F}(f+\varphi_v)$, $v \in V^\perp$, are zero. Then f is not constant on any coset of V. More precisely, since f is three-valued almost optimal, we have for any b:

$$\sum_{v \in V^\perp} (-1)^{b \cdot v} \mathscr{F}(f+\varphi_v) = \pm \lambda 2^{(m+1)/2},$$

where λ is an odd integer, implying that the sum above cannot be zero. In accordance with Lemma 3 we can conclude that f is not affine on any coset of V. This can be seen more generally replacing $V^\perp$ by a coset of $V^\perp$ and applying Lemma 3 again.

Proposition 4. *Let $f \in \mathscr{B}_m$, m odd, be a three-valued almost optimal function; set*

$$Z_f = \{u \mid \mathscr{F}(f + \varphi_u) = 0\}.$$

If for any subspace U of dimension $(m-1)/2$ there exists a such that the cardinality of $Z_f \cap (a + U)$ is odd then f is neither normal nor weakly normal.

By computation, it appears that there are many three-valued almost optimal functions; notably there is a class of such functions which can be decomposed into two bent functions. It is clear that the *concatenation* of two bent functions of $m-1$ variables produces a three-valued almost optimal function of m variables. Conversely if f is such that $D_b f$ is balanced when b describes some hyperplane H, then the restrictions of f to H and to the complement of H are bent functions [4, Theorem V.2]. Recall that a three-valued almost optimal function which is balanced is not normal.

Proposition 5. *Let $f \in \mathscr{B}_m$, m odd, be a three-valued almost optimal function. Let $a \in \mathbf{F}_2^m$ and set $H = \{0, a\}^\perp$. Assume that f has a decomposition with respect to H of the following form*:

$$f(x_1, \ldots, x_m) = (g, h) \text{ where } g \text{ and } h \text{ are bent.}$$

Thus all functions $f + \varphi_v$, $v \in \mathbf{F}_2^m$, have such a decomposition with respect to H. Moreover the following statement are equivalent:

(i) *either f is normal or $f + \varphi_a$ is normal*;
(ii) *g and h are both normal each on some coset of a same subspace of dimension $(m-1)/2$ which is contained in H.*

Proof. As recalled above, f has such a decomposition if and only if $D_b f$ is balanced for all $b \in H$. But $D_b(f + \varphi_v) = D_b f + b \cdot v$, implying that $D_b(f + \varphi_v)$ is balanced as soon as $D_b f$ is balanced. This shows that $D_b(f + \varphi_v)$ is balanced for all $b \in H$, completing the first part of the proof.

Note that $f = (g, h)$ implies $f + \varphi_a = (g, h + 1)$, since H is the kernel of φ_a. Now, we denote by $\bar{H}$ the complement of H. Assume that either f or $f + \varphi_a$ is normal with respect to U, some flat of dimension $(m+1)/2$. This flat is not included in H (or in $\bar{H}$) since otherwise g (or h) would be k-normal with $k = 2^{(m+1)/2}$. According to Theorem 1, this would imply $\mathscr{L}(g) \geqslant 2^{(m+1)/2}$ while $\mathscr{L}(g) = 2^{(m-1)/2}$ because g is bent. So $V = U \cap H$ and $V' = U \cap \bar{H}$ are flats of dimension $2^{(m-1)/2}$. Clearly g is normal with respect to V and h is normal with respect to V'. The case $g\phi_V = h\phi_{V'}$ corresponds to "f is normal" while $g\phi_V \neq h\phi_{V'}$ corresponds to "$f + \varphi_a$ is normal". Obviously, (ii) implies (i), completing the proof. □

Open problem 4. *Construct two bent functions g and h which satisfy: if g and h are normal with respect to U and U', respectively, then U and U' are not cosets of a same subspace.*

4. On normal bent functions

Recall that $f \in \mathscr{B}_m$, m even, is said to be *bent* when its Fourier spectrum contains two values only, $2^{m/2}$ and $-2^{m/2}$. The number of times these values occur is respectively

$$2^{m-1} + (-1)^{f(0)} 2^{m/2-1} \text{ and } 2^{m-1} - (-1)^{f(0)} 2^{m/2-1}.$$

Since f is bent, one can define the *dual function* of f, denoted by $\tilde{f}$:

$$\mathscr{F}(f + \varphi_v) = 2^{m/2}(-1)^{\tilde{f}(v)}, \ v \in \mathbf{F}_2^m.$$

Considering any restriction of f to some subspace, it is related with the restriction of $\tilde{f}$ with the dual of this subspace. More precisely, let V be any subspace of dimension k and let $a \in \mathbf{F}_2^m$. Then (a proof can be found in [5]):

$$\mathscr{F}((\tilde{f} + \varphi_a)\phi_{V^\perp}) = 2^{m/2-k}\mathscr{F}(f\phi_{a+V}). \tag{12}$$

For simplicity, in this section we identify $g\phi_E$, where E is any r-dimensional flat and $g \in \mathscr{B}_m$, to a function of r variables (as explained in Section 2.1).

Now suppose that $k = m/2$ and let $a \in \mathbf{F}_2^m$. Note that for bent functions we find again (10) simply by remarking that for any $v \in V^\perp$:

$$(-1)^{a \cdot v}\mathscr{F}(f + \varphi_v) = 2^{m/2}(-1)^{\tilde{f}(v)+a \cdot v}.$$

The bent function $\tilde{f}(v) + a \cdot v$ is constant on $V^\perp$ if and only if the term on the left is constant when v describes $V^\perp$. More precisely:

Proposition 6. *Let $m = 2t$ and assume that $f \in \mathscr{B}_m$ is bent. We denote by V any subspace of dimension t. Then we have*:

(i) *f is normal with respect to V if and only if its dual function $\tilde{f}$ is normal with respect to $V^\perp$;*
(ii) *f is normal with respect to $a + V$, $a \notin V$, if and only if $\tilde{f} + \varphi_a$ is normal with respect to $V^\perp$;*
(iii) *f is normal with respect to $a + V$, $a \notin V$, if and only if $\tilde{f}$ is weakly normal with respect to $V^\perp$.*

Proof. Note that formula (12) becomes, for $k = t$:

$$\mathscr{F}((\tilde{f} + \varphi_a)\phi_{V^\perp}) = \mathscr{F}(f\phi_{a+V}).$$

Moreover f (resp. $\tilde{f} + \varphi_a$) is normal with respect to $a + V$ (resp. $V^\perp$) if and only if $\mathscr{F}(f\phi_{a+V}) = \pm 2^t$ (resp. $\mathscr{F}((\tilde{f} + \varphi_a)\phi_{V^\perp}) = \pm 2^t$). Thus (i) (for $a = 0$) and (ii) are obviously deduced. Now, $\tilde{f} + \varphi_a$ is normal with respect to $V^\perp$ if and only if there is v such that $\tilde{f} + \varphi_{a+v}$ is weakly normal with respect to $V^\perp$. And these v are those which are not in V. Indeed when $a \notin V$ then the restriction of $x \mapsto a \cdot x$ to $V^\perp$ cannot be

constant; it is of degree 1 exactly. Hence the function $\tilde{f}+\varphi_{a+a}=\tilde{f}$ is weakly normal with respect to $V^{\perp}$. □

The previous proposition leads to an improvement when we want to check if any bent function is normal (or not). Globally, for any V we have only to check f on V and $\tilde{f}$ on $V^{\perp}$ as we precise now.

Corollary 3. *Let $f\in\mathscr{B}_m$, $m=2t$, be a bent function and let $\tilde{f}$ its dual. Let V be a subspace of dimension t. Then f is not normal with respect to any coset of V if and only if $\tilde{f}$ is neither normal nor weakly normal with respect to $V^{\perp}$.*

On the other hand, any bent function is a concatenation of two almost optimal functions whatever the decomposition we choose.

Theorem 3 (Canteaut [4, Theorem V.3]). *Let $f\in\mathscr{B}_m$, $m=2t$, be a bent function. Let H be any hyperplane of $\mathbf{F}_2^m$ and let (f_1,f_2) be the decomposition of f with respect to H. Then f_1 and f_2 are three-valued almost optimal and for any linear Boolean function ℓ (where ℓ can be the null function) of $\mathscr{B}_{m-1}$, we have*

$$\mathscr{F}^2(f_1+\ell)\neq\mathscr{F}^2(f_2+\ell)$$

(i.e. $\mathscr{F}^2(f_1+\ell)=2^m$ if and only if $\mathscr{F}^2(f_2+\ell)=0$).

It apppears again that the normality of bent functions is strongly connected with the normality of three-valued almost optimal functions (see Section 3.2). From now on, $f=(f_1,f_2)$ denotes any decomposition of f as defined in Theorem 3.

Proposition 7. *Let $f\in\mathscr{B}_m$, $m=2t$, be a bent function. Let V be a subspace of dimension t and let H be any hyperplane containing V. Let $f=(f_1,f_2)$ be the decomposition of f with respect to H.*

Then f is normal with respect to some coset of V, say $a+V$, if and only if either $a\in H$ and f_1 is normal with respect to $a+V$ (when $\mathscr{F}(f_1)\neq 0$) or $a\notin H$ and f_2 is normal with respect to $a+V$ (when $\mathscr{F}(f_2)\neq 0$).

Proof. From Theorem 3, we know that $\mathscr{F}^2(f_1)\neq\mathscr{F}^2(f_2)$. So we can assume that $\mathscr{F}(f_1)\neq 0$ and $\mathscr{F}(f_2)=0$; otherwise we consider the translated function $g=(f_2,f_1)$. Recall that $\mathscr{L}(f_1)=\mathscr{L}(f_2)=2^{m/2}$.

Suppose that f is normal with respect to $a+V$. Since $V\subset H$, either f_1 or f_2 is constant on $a+V$. As the dimension of V equals $m/2$ and $f_i\in\mathscr{B}_{m-1}$, "constant" means "normal" here. But, according to Theorem 1, f_2 cannot be normal since it is balanced. Hence $a+V$ is included in H and f_1 is normal. The inverse statement is obvious. □

As an illustration, we can extend Proposition 3 to functions of 8 variables.

Proposition 8. *For $m = 8$, any bent function which has at least one affine derivative is normal. In particular, any cubic bent function of 8 variables is normal.*

Proof. Let $f \in \mathscr{B}_8$ be a bent function. Assume that there is at least one direction a, $a \neq 0$, such that $D_a f$ is affine. Thus $D_a f = \varphi_b + \varepsilon$ for some b, $\varepsilon \in \{0,1\}$. Note that $D_a f$ cannot be constant since f is bent. Let H be the hyperplane $\{0,b\}^\perp$. In this case the decomposition of f with respect to H is as follows: $f = (f_1, f_2)$ where $D_a f_1 = D_a f_2 + 1 = 0/1$ (see more in [5]).

Actually f_1 and f_2 are almost optimal functions which have a linear structure; they are partially bent. Moreover, either f_1 or f_2 is not balanced. Assuming that f_1 is not balanced, then f_1 is normal while f_2 is weakly normal only (according to Proposition 3). From Proposition 7, f is normal.

Cubic bent functions of eight variables were classified by Hou in [15]. It appears that all these functions have an affine derivative.[3] □

Open problem 5. *Does it exist non-normal bent functions of 8 variables and degree 4?*

Now consider any decomposition $f = (f_1, f_2)$ with respect to $H = \{0,b\}^\perp$ for some b. Let V be a subspace of dimension $t = m/2$ not included in H; so the dimension of $V' = V \cap H$ equals $t-1$. If f is normal with respect to $a + V$ then f_1 and f_2 are $(t-1)$-normal each with respect to a coset of V'. Conversely, if f_1 and f_2 are $(t-1)$-normal each with respect to some coset of V' then f is either normal or (if the considered restrictions of f_1 and f_2 are not equal) weakly normal. So, in accordance with Proposition 7, we can conclude

Proposition 9. *Let $f \in \mathscr{B}_m$, $m = 2t$, be a bent function which is neither normal nor weakly normal. Let $f = (f_1, f_2)$ be any decomposition of f with respect to some hyperplane H. Then f_1 and f_2 are neither normal nor weakly normal. Moreover, if f_1 is $(t-1)$-normal with respect to a coset of some subspace V' this property does not hold for f_2.*

Open problem 6. *Characterize $f \in \mathscr{B}_m$, $m = 2t-1$, which is three-valued almost optimal and not $(t-1)$-normal.*

Appendix

As an illustration, we study here the normality of quadratic Boolean functions. We state that any quadratic function is constant on several flats and notice that only one kind of such functions is not normal. Recall that any quadratic function $f \in \mathscr{B}_m$ has a unique representation, up to an affine transformation on the variables (see, for

[3] This happens for $m = 8$ only, as proved Canteaut and Charpin later [5].

instance, [16, p. 438]). It is

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{h} x_{2i-1}x_{2i} + \left(\sum_{j=h+1}^{(m-\varepsilon)/2} (\lambda_j x_{2j-1} + \mu_j x_{2j}) \right) + v x_m + \tau, \qquad (A.1)$$

where

- $\lambda_j,\ \mu_j \in \mathbf{F}_2,\ \tau \in \{0,1\}$,
- by convention $[h+1, (m-\varepsilon)/2]$ is empty when $h = (m-\varepsilon)/2$,
- $\varepsilon = 0$ for even m and $\varepsilon = 1$ for odd m,
- $v = 0$ for even m and $v \in \mathbf{F}_2$ for odd m.

It is well-known that the values of the Fourier spectrum of f are $\{0, \pm 2^{m-h}\}$ when $2h < m$ and $\{\pm 2^{m/2}\}$ when $h = m/2$—i.e., m is even and f is bent.

Theorem A.1. *Let $f \in \mathscr{B}_m$, $m \geqslant 4$, be any quadratic function with non-linearity 2^{m-h}, $1 < h \leqslant \lfloor m/2 \rfloor$. Then f is normal except when m is odd, $h = (m-1)/2$, and f has the following form (up to equivalence):*

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{(m-1)/2} x_{2i-1}x_{2i} + x_m + \tau,\ \tau \in \{0,1\}. \qquad (A.2)$$

In this case, f is not normal but weakly normal.

More generally, when $h < \lfloor m/2 \rfloor$ then f is k-normal, with $k = m - (h+1)$, with respect to several k-dimensional flat.

Proof. We consider form (A.1) of f. We can assume $\tau = 0$ without loss of generality. We first suppose that $h < (m-\varepsilon)/2$. Let V be the subspace of $\mathbf{F}_2^m$ defined by

$$x_2 = x_4 = \cdots = x_{2h} = 0 \text{ and } \sum_{j=h+1}^{(m-\varepsilon)/2} (\lambda_j x_{2j-1} + \mu_j x_{2j}) + v x_m = 0.$$

Clearly V has dimension $k = m - (h+1)$. Moreover $f(x) = 0$ for any $x \in V$. Hence f is k-normal with respect to V. Note that we can do other choices for the h equations above on the left, completing the last part of the proof. Therefore f is normal with respect to any affine subspace of V of dimension $\lceil m/2 \rceil$.

When m is even and $h = m/2$ we define V, for instance, by

$$x_2 = x_4 = \cdots = x_{2h} = 0.$$

Thus f is normal with respect to V whose dimension is $m/2$. Now suppose that m is odd and $h = (m-1)/2$. In this case f satisfies $\mathscr{L}(f) = 2^{(m+1)/2}$, its spectrum is $\{0, \pm 2^{(m+1)/2}\}$ and its form is

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{(m-1)/2} x_{2i-1}x_{2i} + v_m x_m.$$

Note that f is three-valued almost optimal (see Definition 6). Consider V, the subspace of dimension $(m+1)/2$ defined by $x_2 = x_4 = \cdots = x_{2h} = 0$. Clearly f is either constant ($v = 0$) or linear ($v = 1$) on this subspace. When $v = 1$, f is balanced since for $a = (0, \ldots, 0, 1)$

$$D_a f(x) = x_m + (x_m + 1) = 1.$$

From Theorem 1, f is not normal. □

References

[1] P. Camion, C. Carlet, P. Charpin, N. Sendrier, On correlation-immune functions, in: Advances in Cryptology—CRYPTO'91, Lecture Notes in Computer Science, Vol. 576, Springer, Berlin, 1991, pp. 86–100.
[2] A. Canteaut, Private communication.
[3] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions, in: Advances in Cryptology—EUROCRYPT 2000, Lecture Notes in Computer Science, Vol. 1807, Springer, Berlin, 2000, pp. 507–522.
[4] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, On cryptographic properties of the cosets of $R(1,m)$, IEEE Trans. Inform. Theory 47 (4) (2001) 1494–1513.
[5] A. Canteaut, P. Charpin, Decomposing bent functions, IEEE Trans. Inform. Theory 49 (2003) 2004–2019.
[6] A. Canteaut, M. Daum, G. Leander, H. Dobbertin, Normal and non normal bent functions, in: Proceedings of the 2003 International Workshop on Coding and Cryptography (WCC 2003), Versailles, France, March 2003, pp. 91–100.
[7] C. Carlet, Partially-bent functions, Des. Codes Cryptogr. 3 (1993) 135–145.
[8] C. Carlet, On the complexity of cryptographic Boolean functions, in: Sixth International Conference on Finite Fields and Applications, Lecture Notes in Computer Science, Springer, Berlin, 2002, pp. 53–69.
[9] C. Carlet, A larger class of cryptographic Boolean functions via a study of the Maiorana–McFarland construction, in: Advances in Cryptology—CRYPTO 2002, Lecture Notes in Computer Science, Vol. 2442, Springer, Berlin, 2002, p. 549 ff.
[10] P. Charpin, E. Pasalic, On propagation characteristics of resilient functions, in: Selected Areas in Cryptography—SAC 2002, Lecture Notes in Computer Science, Vol. 2595, Springer, Berlin, 2003, pp. 356–365.
[11] M. Daum, G. Leander, H. Dobbertin, An algorithm for checking normality of Boolean functions, in: Proceedings of the 2003 International Workshop on Coding and Cryptography (WCC 2003), March 2003, pp. 133–142.
[12] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, in: Fast Software Encryption, Lecture Notes in Computer Science, Vol. 1008, Springer, Berlin, 1994, pp. 61–74.
[13] S. Dubuc, Etude des propriétés de dégénérescence et de normalité des fonctions booléennes et construction de fonctions q-aires parfaitement non-linéaires, Ph.D. Thesis, Université de Caen, 2001.
[14] C. Fontaine, On some cosets of the first-order Reed–Muller code with high minimum weight, IEEE Trans. Inform. Theory 45 (4) (1999) 1237–1243.
[15] X.-D. Hou, Cubic bent functions, Discrete Math. 189 (1998) 149–161.
[16] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[17] N.J. Patterson, D.H. Wiedemann, The covering radius of the $[2^{15}, 16]$ Reed–Muller code is at least 16276, IEEE Trans. Inform. Theory IT-36 (2) (1983) 443.

[18] P. Sarkar, S. Maitra, Nonlinearity bounds and constructions of resilient Boolean functions, in: Advances in Cryptology—CRYPTO 2000, Lecture Notes in Computer Science, Vol. 1880, Springer, Berlin, 2000, pp. 515–532.
[19] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Trans. Inform. Theory IT-30 (5) (1984) 776–780.
[20] Y. Tarannikov, On resilient Boolean functions with maximal possible nonlinearity, in: Proceedings of Indocrypt 2000, Lecture Notes in Computer Science, Vol. 1977, Springer, Berlin, 2000, pp. 19–30.

Further reading

J.F. Dillon, Elementary hadamard difference sets, Ph.D. Thesis, University of Maryland, 1974.